The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

09/10/2013

SUBJECT:

Vulnerability In OLE Could Allow Remote Code Execution (MS13-070)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE), which could allow an attacker to take complete control of an affected system. Microsoft OLE allows an application to link part of a document to another application of a different type for processing.

The vulnerability could allow remote code execution if a user opens a specially crafted file. Successful exploitation of this vulnerability could allow the attacker to could gain the same user rights as the current user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE). This remote code execution vulnerability exists due to the way Microsoft Windows handles OLE objects in memory. The vulnerability could allow remote code execution if a user opens a file that contains a specially crafted OLE object. Successful exploitation of this vulnerability could allow the attacker to could

gain the same user rights as the current user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/security/bulletin/ms13-070

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3863